AMENDMENTS TO THE CLAIMS

Please accept amended Claims 1, 22, and 23, and new Claim 29 as follows.

Listing of claims.

1-10. (Cancelled)

11. (Currently Amended) A method for ensuring that a processor will execute only authorized boot code, said method comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized boot code into said protected memory, wherein said protected memory is cryptographically protected;

~~verifying~~ reading, by said processor, a digital signature used to sign said signed authorized boot code;

decrypting said digital signature to generate a decrypted digital signature;

verifying said decrypted digital signature in accordance with said first public key;

executing, by ~~the~~ said processor, said signed authorized boot code having a verified digital signature by branching to ~~a copy of~~ said signed authorized boot code in said protected memory, said signed authorized boot code including instructions for performing a boot process for a computer device comprising ~~the~~ said processor, wherein said digital signature of said signed authorized boot code is previously verified and executing further comprises performing inline decryption of the copy of said signed authorized boot code in said protected memory.

12. (Cancelled)

13. (Previously Presented) A method as recited in claim 11 wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor.

14. (Original) A method as recited in claim 11 wherein said protected memory is physically protected.

15. (Cancelled)

16. (Previously Presented) A method as recited in claim 11 wherein the integrity of said authorized boot code is protected at run time.

17. (Previously Presented) A method as recited in claim 16 wherein the integrity of said authorized boot code is protected with symmetric key encryption.

18. (Previously Presented) A method as recited in claim 11 wherein the privacy of said authorized boot code is protected at run time.

19. (Previously Presented) A method as recited in claim 18 wherein the privacy of said authorized boot code is protected at run time with symmetric key encryption.

20-21. (Cancelled)

22. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized boot code into said protected memory, wherein said protected memory is cryptographically protected;

~~verifying~~ reading, by said processor, a digital signature used to sign said signed authorized boot code;

decrypting said digital signature to generate a decrypted digital signature;

verifying said decrypted digital signature in accordance with said first public key;

executing said signed authorized boot code having a verified digital signature by branching to ~~a copy of~~ said signed authorized boot code in said protected memory, said signed authorized boot code including instructions for performing a boot process for a computer device comprising ~~the~~ said processor, wherein said digital signature of said signed authorized boot code is previously verified and executing further comprises performing inline decryption of the copy of said signed authorized boot code in said protected memory.

23. (Currently Amended) A computing device for securely executing authorized code, said computing device comprising:

a protected memory for storing a signed authorized boot code, which contains ~~an original~~ a digital signature, wherein said protected memory is cryptographically protected; and a processor comprising inline cryptography and integrity hardware for executing said signed authorized boot code, said processor in signal communication with said protected memory, said processor reading and decrypting said signed authorized boot code from the protected memory and executing said signed authorized boot code from the protected memory for booting the computing device after verifying that ~~a~~ said digital signature contained in said signed authorized boot code is ~~original~~ valid as decrypted in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor, and branching to ~~a copy of~~ said signed authorized boot code in said protected memory to begin the execution.

24. (Previously Presented) A computing device as recited in claim 23 wherein the integrity of the contents of said protected memory is protected by encryption.

25. (Previously Presented) A computing device as recited in claim 23 wherein said protected memory is physically protected.

26. (Previously Presented) A computing device as recited in claim 23 wherein at least one of the integrity of said authorized code and the privacy of said authorized code is protected at run time.

27. (Previously Presented) A computing device as recited in claim 23 wherein the integrity of said signed authorized code is protected at run time with symmetric key encryption.

28. (Previously Presented) A computing device as recited in claim 23, wherein the privacy of

said signed authorized code is protected at run time with symmetric key encryption.

29. (New) A computing device as recited in claim 23, where said processor further comprises:

a first summing block summing said read copy of said signed authorized boot code from the protected memory with a whitening value;

a decryption block decrypting an output of said first summing block;

a second summing block summing an output of said decryption block with said whitening value to generate plaintext data corresponding to said copy of said signed authorized boot code from said protected memory; and

a function block validating said plaintext data for execution.